The ElGamal cryptosystem

Alice | **Bob**

g → $g \in \mathbb{F}_q^*$: generator (or element of high order) in large finite field $\mathbb{F}_q$

Chooses secret element $a \in \mathbb{F}_q^*$

Chooses secret element $b \in \mathbb{F}_q^*$

Sends public key g^a → g^a

Writes message with blocks $M \in \mathbb{F}_q^*$

g^b and $M \cdot g^{ab}$ ← Sends g^b and $M \cdot (g^a)^b$

Common secret key

Deciphers using her secret key a:

$(g^b)^a = g^{ba} = g^{ab}$

She computes the multiplicative inverse of $(g^b)^a$ and takes its product with $M \cdot g^{ab}$

$$(g^a)^b = (g^b)^a$$

Example for the ElGamal cryptosystem

Alice | **Bob**

Picks the generator $g=35$ of $(\mathbb{Z}/3593\mathbb{Z})^*$ ⟼ $g=35$, $p=3593$

Chooses secret key $a=16$

Chooses secret key $b=8$

Sends public key g^a

$35^{16} = 507094277490249633789625$

$\equiv 2312 \bmod 3593$ ⟼ 2312

Pads message block „HI" into 481.

$g^b \equiv 639$ ⟵ Sends $g^b \equiv 639 \bmod 3593$

$(g^b)^a = (639)^{16} \equiv 670 \bmod 3593$

Exponentiates $(g^a)^b = (2312)^8 \equiv 670 \bmod 3593$

Ciphertext for 2493 $(x=0, y=42, z=15)$ „lO" ⟵ Multiplies $481 \cdot (g^a)^b \equiv 2493 \bmod 3593$

$((g^b)^a)^{-1} = \frac{1}{670} \equiv 1035 \bmod 3593$

Multiplies

$1035 \cdot 2493 \equiv 481 \bmod 3593$

Unpads 481 via $8 \cdot 59 + 9$ into „HI".

Mini-example for the ElGamal cryptosystem

Alice | **Bob**

Picks generator $g=2$ of $(\mathbb{Z}/11\mathbb{Z})^*$ ⟷ $g=2$, $p=11$

Chooses secret key $a=3$

Chooses secret key $b=5$

Sends public key $g^a \equiv ? \bmod 11$ ⟷ $? \equiv g^a$

g^b ⟵ Sends $g^b \equiv ? \bmod 11$

Wants to send secret message $M=9$

$(g^b)^a \equiv ? \bmod 11$

$((g^b)^a)^{-1} \equiv ? \bmod 11$

Eponentiates $(g^a)^b \equiv ? \bmod 11$

$(g^a)^b \cdot M$ ⟵ Multiplies $M \cdot (g^a)^b \equiv ? \bmod 11$

$((g^b)^a)^{-1} \cdot M \cdot (g^a)^b \overset{\nabla}{\equiv} M \bmod 11$